

IN THE UNITED STATES DISTRICT COURT
FOR MARYLAND

✓ FILED _____ ENTERED
_____ LOGGED _____ RECEIVED
12:44 pm, Oct 19 2020
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

**IN THE MATTER OF THE SEARCH OF
ASSOCIATED WITH THE FOLLOWING
CELLULAR DEVICES:**

iPhone – ATF Property Item #012
Samsung – ATF Property Item #013
TCL – ATF Property Item #014

(“TARGET CELLULAR DEVICES”)

Case No. 1:20-mj-2380 TMD

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Jenna L. Klausung, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Baltimore Field Office, Annapolis RA, Annapolis, MD, (hereinafter the “Affiant”) being duly sworn, deposes and states as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41. This warrant would authorize investigators to search the **TARGET CELLULAR DEVICES** (as described in Attachment A) for the items described in Attachment B.

2. Your Affiant is “a federal law enforcement officer” within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a government agent who is engaged in enforcing the criminal laws and who is in a category of officers authorized by the Attorney General to request a search warrant. I have been employed with the FBI since October of 2019. Since March of 2020, I have been assigned to work federal investigations of a violent criminal nature. Prior to my employment with the FBI, I served in the United States Army as a Military Police Officer, conducting investigations ranging from financial liability to various forms of

soldier misconduct. Since 2016, I have received training and experience in interviewing and interrogation techniques, arrest procedures, search and seizure, and other forms of violent crime. I have further received training and experience since 2019 through the FBI regarding geolocation and data exploitation as well as the role mobile devices play in various forms of crime. During my training and experience, I have become familiar with the requirements for probable cause. I also have training and experience in the enforcement of laws of the United States, including training in the preparation and execution of search warrants. I have also assisted in the preparation and/or execution of numerous search and arrest warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my knowledge, training, and experience, I know that individuals involved with acts of arson frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities and to conduct research various incendiary devices. Additionally, based upon knowledge, training, and experience, and participation in this and other arson investigations, I know the following:

a. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. Cellular phones have both digital storage capacity and digital camera capabilities.

b. Cell phone users take, store, and post photographs of themselves and others, which can be used to identify the perpetrators (for example, by matching the clothing being worn

by perpetrators on surveillance videos with clothing worn by the account user in social media posts), and photograph their potential targets, which can provide a link between the perpetrator and the crime. In addition, location data can be stored in photographs' exchangeable image file (EXIF) data and metadata, which could provide evidence to prove **CORENLIUS JAQUEZ HENDRIX's** (herein referred to as "**HENDRIX**") locations at times relevant to this investigation.

c. Individuals who engage in arson and/or who build homemade incendiary devices often conduct online research into how to commit these offenses, sometimes months in advance of the crime. This research can include written materials, manual, photographs, and videos available online, which may be stored in the **TARGET CELLULAR DEVICES'** documents, the internet browser's history, or messages sent between co-conspirators.

d. Cellular telephones use Internet Protocol addresses to access the internet and geolocation data through the connection of cellular towers, mapping features and data applications can provide information regarding the whereabouts of subjects in relation to locations of illegal activity.

5. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. 844 (i), Damage by means of fire real property affecting interstate commerce, 18 U.S.C. 844(h)(1), Use of fire or an explosive to commit any felony that may be prosecuted in a court of the United States (the "**TARGET OFFENSES**") have been committed by **HENDRIX**. There is also probable cause to believe that the **TARGET CELLULAR DEVICES** used by **HENDRIX** will contain evidence of those criminal violations. This information may constitute evidence of the crimes under investigation, because the information can be used to identify any associates of **HENDRIX** and

may reflect the nature of scope of the intended crime as well as identify the subjects' motives for committing these offenses.

PROBABLE CAUSE

6. On August 21, 2020 at approximately 0523AM, Fort Meade Emergency Services received a 9-1-1 call reporting a fire at 1836 Sidman Court, Unit 4, Fort Meade, Maryland. Fort Meade Fire Department (FMFD) Deputy Fire Chief James Evans responded to the fire scene and reported a small, extinguished fire inside Unit 4. Some smoldering carpet on the second floor was fully extinguished with a water can. The Unit was occupied by the following persons at the time of the fire: Stacy Hendrix, Mary Hendrix, **(CORNELIUS) HENDRIX**, and a juvenile. On this same date, Special Agent Certified Fire Investigator (SACFI) James McKinnies was contacted by ATF Task Force Officer Carroll Spriggs and asked to respond to the fire scene to assist the Anne Arundel County (AACo) Fire Investigation Unit and the Fort Meade Military Police Department (FMMP) with the fire investigation due to the location of the fire scene on the Military Installation.

7. On August 21, 2020, **HENDRIX** received medical treatment for an injured leg, incurred by jumping off the rear porch roof of the residence. Later on August 21, 2020, **HENDRIX** was discharged from the Baltimore Washington Medical Center. At that time, law enforcement took custody of property that **HENDRIX** had upon admission to the Medical Center, which included the **TARGET CELLULAR DEVICES**. Continuing on August 21, 2020, following **HENDRIX**'s discharge from the Medical Center, SACFI McKinnies and Special Agent Sean Regan of the Federal Bureau of Investigation (FBI) interviewed **HENDRIX** at the FMMP.

8. During this interview, **HENDRIX** admitted to investigators he had set the fire at the location in question (1836 Sidman Court, Unit 4, Fort Meade, MD). **HENDRIX** stated he was hearing voices in his head that told him to "hurt people that hurt him". **HENDRIX** admitted to

utilizing lighter fluid to start the fire. In conjunction with **HENDRIX**'s statements, fire debris was discovered and documented in the second-floor hallway and on the ground floor near an entrance of the home. Furthermore, a bottle of charcoal lighter fluid and a lighter was found in the backyard.

9. **HENDRIX** was transported from FMMP on August 22, 2020, to the FBI Baltimore Field Office where he was interviewed by SACFI McKinnies and SA Regan. Over the course of the interview, **HENDRIX** admitted again to setting the fire in his father and stepmother's home (1836 Sidman Court, Unit 4, Fort Meade, MD). **HENDRIX** stated he utilized lighter fluid and a lighter to start the fire. **HENDRIX** stated he acquired the lighter fluid and lighter from the covered patio area of the residence. **HENDRIX** further stated how he first started the fire upstairs on the carpet and on the doors, then moved downstairs, spraying the stairs and the inside of the downstairs door on the inside with lighter fluid. **HENDRIX** stated he then threw the lighter and the lighter fluid into the backyard area. **HENDRIX** explained that he had also thought of poisoning his stepmother with Clorox, possibly in her drink.

10. SACFI McKinnies concluded that the fire was incendiary, that is, intentionally set where a fire should not be.

11. On August 22, 2020, **HENDRIX** was arrested on a single count of 18 U.S.C. § 844(i). Case No. 20-2174 ADC. The **TARGET CELLULAR DEVICES** which were recovered at the Medical Center were secured, and have been in the custody of law enforcement since that time. The **TARGET CELLULAR DEVICES** are presently secured with the ATF. To date, no effort has been made to forensically examine the contents of the **TARGET CELLULAR DEVICES**.

12. Your Affiant submits that there is probable cause to forensically examine the **TARGET CELLULAR DEVICES** as evidence of travel, photographs or video prior to or

immediately after commission of the **TARGET OFFENSES**, as well as communications and/or search terms that may show planning by **HENDRIX** alone or with others to commit the **TARGET OFFENSES** or efforts to avoid detection/apprehension immediately thereafter.

CONCLUSION

13. Based on the foregoing, I have probable cause to believe, and I do believe, that **HENDRIX** committed the **TARGET OFFENSES** and that evidence of those offenses are presently contained in the **TARGET CELLULAR DEVICES**, which is more fully described above and in Attachment A hereto. Therefore, I respectfully request that the attached warrant be issued authorizing the search of the **TARGET CELLULAR DEVICES** identified in Attachment A and to seize any items located pursuant to the search as defined in Attachment B, incorporated by reference, for evidence of the **TARGET OFFENSES**.

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this ____ day of September, 2020.

Jenna Klausning

Jenna Klausning
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on: September 22, 2020

Thomas M. DiGirolamo

Honorable Thomas M. DiGirolamo
United States Magistrate Ju

ATTACHMENT A
Property to be Searched

The property to be searched is the **TARGET CELLULAR DEVICES:**

- 1) iPhone – ATF Property Item #012
- 2) Samsung – ATF Property Item #013
- 3) TCL – ATF Property Item #014

ATTACHMENT B
Items to be Seized

All records contained on the **TARGET CELLULAR DEVICES** further described in Attachment A which constitute evidence of violations of 18 U.S.C. § 844 (i) (Damage by means of fire real property affecting interstate commerce), and 18 U.S.C. § 844(h)(1) (Use of fire or an explosive to commit any felony that may be prosecuted in a court of the United States) (the “**TARGET OFFENSES**”), as outlined below:

1. All digital images; records of incoming and outgoing voice communications; records of incoming and outgoing text communications; the content of incoming and outgoing text communications; voicemails; voice recordings; contact lists; records of Internet Protocol addresses used; any information recording **HENDRIX**’s schedule or travel on or around August 21, 2020; records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
2. Any and all records related to the location of the user(s) of the devices.
3. For each of the **TARGET CELLULAR DEVICES**:
 - a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the **TARGET CELLULAR DEVICES** of other storage devices or similar containers for electronic evidence;

- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the **TARGET CELLULAR DEVICES**;
- f. evidence of the times the **TARGET CELLULAR DEVICES** were used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the **TARGET CELLULAR DEVICES**;
- h. documentation and manuals that may be necessary to access the **TARGET CELLULAR DEVICES** or to conduct a forensic examination of the **TARGET CELLULAR DEVICES**;
- i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including **TARGET CELLULAR DEVICES**), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
2. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
3. “scanning” storage areas to discover and possibly recover recently deleted files;
4. “scanning” storage areas for deliberately hidden files; or
5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically

stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.